**Report (Word Document):**

Using what you know about the company from this case study, create a report with your audit findings, making sure to include responses to the questions below: **(NOTE: The questions below are in no significant order. Make sure to review each and include in a format that makes sense to the executives. Since this document is going to the CIO of the company, make sure to include a table of contents and Executive Summary section.)**

* Does the company use a defense in depth or layered defense approach to Information Security based on knowledge of policies, practices, and network design?
  + Does the provided network diagram adequately use these approaches for technical controls inside a corporate organization? What could they do differently to improve the network’s overall security? Are there additional technical controls needed?
* What is a DMZ? Could this company benefit from the use of one? If so, what assets should be placed in the DMZ?
* What threats and vulnerabilities does this company face given their current Information Security posture?
* What type of data does the company process? What types of laws/regulations/compliance does the company have to abide by?
* Is there any risk of exposure to credit card number theft?
* How can Information Security posture become better in the organization?
* How should the company address risk issues and assessments?
* How can policies and procedures inside the company be altered to benefit processes and positively impact emergency downtimes and procedures?
* Are the policies that you have created for the company part of an Enterprise (Program) Information Security Policy, Issue-Specific Security Policy, or System Specific Policy?
* What type of communication should this company encrypt? Should they encrypt data at rest, data in transit, or both? Why? How should policies for data encryption be handled?
* What can the company use to handle business continuity in the event of a disaster? Given the maximum tolerable downtimes for critical systems, what steps/processes/technology can the IT department ensure optimal recovery times?
  + Given some of these critical systems, what should backups and data retention policies be for these? Remember to take into account the company’s physical location (Headquarters).
* What is the basis for your audit suggestion and the purpose and justification for them? What problem/issue/risk will they be resolving?